Annual 47 C.F.R. S: 64.2009(e) CPNI Certification
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for:	2015, covering prior year 2014
Date filed:	February 11, 2015
Name of the Company covered by this certification:	Alliant Technologies, LLC
Form 499 Filer ID:	830170
Name of signatory:	Bruce Flitcroft
Title of signatory:	CEO

I, Bruce Flitcroft, certify that I am an officer of Alliant Technologies, LLC, and acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. S: 64.2001 et seq., which is a subpart to implement **section 222 of the Communications Act of 1934 as amended, 47 U.S.C. 222**.

Attached to this certification is an accompanying statement explaining how the Company's procedures ensure that the Company is in compliance with the requirements set forth in section 64.2001 et seq. of the Commission's rules. See attached accompanying statement for details.

The Company **has not had to take any actions** in the form of proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers against in the past year. The Company understands that it must report on any information that it has with respect to the processes pretexters are using to attempt to access CPNI, and what steps the Company is taking to protect CPNI.

Note, the Company recognizes "pretexting" as **"the process in which personal information is obtained by fraudulent means including identity theft, selling personal data for profit, or using some other method for snooping for information whose release was not authorized by the owner of the information." See the attached accompanying statement for details on how the Company guards CPNI data against pretexting.**

The Company has received **0** customer complaints related to unauthorized access of CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint as follows:

(1). Instances of improper access by employees: **0 Complaints**
(2). Instances of improper disclosure to individuals not authorized to receive the information: **0 Complaints**
(3). Instances of improper access to online information by individuals not authorized to view the information. **0 Complaints**

If there were any complaints listed above, the Company would attach a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. The Company is aware of "Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services, CC Docket No. 96-115; WC Docket No. 04-36,

Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007)("EPIC CPNI Order"). See 47 U.S.C. S: 222"

The Company understands "47 C.F.R. S: 64.2009(e) in that it states:

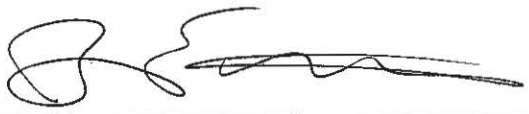
(1). "A telecommunications carrier must have an officer, as an agent of the carrier, sign and file with the Commission a compliance certificate on an annual basis.

(2). That the officer must state in the certification that he or she has personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the rules in this subpart.

(3). That the carrier must provide a statement accompanying the certification explaining how its operating procedures ensure that it is or is not in compliance with the rules in this subpart.

(4). That the carrier must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI.

(5). That this filing must be made annually with the Enforcement Bureau on or before March 1 in EB Docket No. 06-36, for data pertaining to the previous calendar year."

Signed X  [signature]

Attached CPNI Accompanying Statement pg 1 of 3

The following are the measures put in place by the carrier (herein referred to as "the Company") to protect CPNI from pretexting. The Company understands that the three common types of "pretexting" are **identity theft, selling personal data for profit without authorization by the owner** or **using some other method for snooping for information whose release was not authorized by the owner of the information.**

I. Pretexting via identity theft

(A). Identity theft via theft of physical hardware containing CPNI Data

Guarding Measures:

The Company utilizes physical security such as locks and security surveillance to protect physical hardware and limits physical access to authorized personnel. Also, certain portable hardware such as laptops have security features such as data encryption that provide additional security.

(B). Identity theft via hacking/virtual intrusion of systems that carry CPNI.

Guarding Measures:

The Company uses network security devices and software to detect and prevent unauthorized access via hacking and other virtual access methods.

II. Pretexting via some other method for snooping for information whose release was not authorized by the owner

(A). Snooping by external personnel via social engineering/ impersonation/false identification

Guarding Measures:

The Company's customer service personnel do not have access to this information, and those personnel that do have access to this information have specific policies they must follow to identify that they are in contact with the owner of the CPNI data prior to discussing or revealing CPNI.

(B). Snooping by personnel not authorized to access data

Guarding Measures:

The Company limits access of CPNI to authorized personnel only.

III. Pretexting by selling CPNI for profit without authorization by the owner

(A). Selling CPNI data by the Company to other companies

Guarding Measures:

The Company does not sell CPNI data to other companies for any purpose.

(B). Sharing CPNI data for profit/marketing purposes by the Company with business partner, subsidiary, sibling or parent companies or joint venture entities.

Guarding Measures:

Detailed as items 1 to 9 on the following pages.

Attached CPNI Accompanying Statement pg 2 of 3

The following items (1) to (9) are how The Company guards CPNI against pretexting in the form of sharing CPNI for profit or marketing purposes by The Company with its business partner, subsidiary, sibling or parent companies or joint venture entities without authorization by the CPNI owner. In the event that the Company was to sell or share CPNI with its affiliated entities for marketing or profit purposes, it would strictly abide by the following policies in compliance with FCC rules as outlined in section 222 of the Communications Act of 1934 as amended, 47 U.S.C. 222 (47 C.F.R. S: 64.2001 to 64.2011 et seq.).

How The Company Complies with 47 C.F.R. S: 64.2001-64.2011 et seq.

(1). The Company does not enable use, disclosure or permit access to CPNI for any marketing purposes to any persons, entities parties outside of the Company without the specific consent of the customer that owns the CPNI data.
(2). The Company will secure a written or electronically signed consent from a customer before sharing CPNI data with any Business Partner, Subsidiary, Parent or Sibling companies regardless of how many services the customer subscribes to.
(3). The Company will not utilize, disclose or permit access to CPNI data to identify or track customers that call competing service providers.
(4). If the Company requires customer consent for utilizing, disclosing or permitting access to CPNI data, the Company will obtain consent through written or electronic methods, and not use any oral consent methods.
(5). The Company has a policy in which any customer approvals obtained for the use, disclosure or utilization of CPNI data will remain in effect until the customer revokes or limits such approval or disapproval.
(6). The Company only uses a written or electronic approval processes relying on a physically or electronically signed consent form, and does not use any other opt-out or opt-in method for CPNI.
(7). Prior to any solicitation of the customer for approval, the Company provides notification to the customer of the customer's rights to restrict to use of, disclosure of, and access to that customer's CPNI.
(8). The Company maintains records of notification, written or electronic, for at least one year. The Company provides individual notices to customers when soliciting approval to use, disclose or permit access to customer's CPNI.

Attached CPNI Accompanying Statement pg 3 of 3

(9). In cases where the Company requests CPNI release consent from the customer, the Company includes the following in its **"Consent Notice"**

I. Sufficient information to enable the customer to make an informed decision as to whether to permit the Company to use, disclose or permit access to, the customer's CPNI.

II. Statement declaring that the customer has a right, and that the Company has the duty, under federal law, to protect the confidentiality of CPNI.

III. Specific statement on that the types of information that constitute CPNI (**as defined in 64.2001**) and the specific entities that will receive the CPNI, describing the purposes for which CPNI will be used, and inform the customer of his or her right to disapprove those uses, and deny or withdraw access to CPNI at any time.

IV. Statement advising the customer of the precise steps the customer must take in order to grant or deny access to CPNI, and clear statement that a denial of approval will not affect the provision of any services to which the customer subscribes. The Company also provides a brief statement, in clear and neutral language, describing consequences directly resulting from the lack of access to CPNI. The Company's notification will be comprehensible and not be misleading.

V. In cases where the Company utilizes written notification, the notice will be clear, legible, sufficiently large type and be placed in an area so as to be readily apparent to a customer.

VI. In the event that the notification is to be translated into another language, then all portions of the Company's notification will be translated into that language.

VIII. The Company will not include in the notification any statement attempting to encourage a customer to freeze third-party access to CPNI.

IX. The notification will state that any approval, or denial of approval for the use of CPNI outside of the service to which the customer already subscribes from the Company is valid until the customer affirmatively revokes or limits such approval or denial.

X. The Company's solicitation for approval will state the customer's CPNI rights (defined in **47 C.F.R. S: 64.2001 to 64.2011 et seq.).**